Robust Data Exchange across Wind Turbines

Xian Liu
Department of Systems Engineering
University of Arkansas at Little Rock
Little Rock, USA
xxliu@ualr.edu

Changcheng Huang
Department of Systems and Computer Engineering
Carleton University
Ottawa, Canada
huang@sce.carleton.ca

2023 5th International Conference on Computer Communication and the Internet (ICCCI) | 979-8-3503-2695-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCCI59363.2023.10210105

***Abstract*—Wind farms play an important role in the smart grid initiative. Most wind turbines are deployed in open areas and their wireless communication layer needs to be robust. In this paper, the concept of information-theoretic secrecy is introduced to establish some benchmarks of robust communication. Compatible with the common topology of wind turbine deployment, the secrecy analysis is conducted in the framework of cooperative communication with a generic relay configuration. The analysis takes several issues into account, such as fading, line-of-sight, and multi-scattering. We derive several benchmark metrics for this system. These metrics are explicitly expressed in the closed-form. The availability of these solutions helps directly gain the deep insights, while reducing the computational load of tedious simulations.**

***Index Terms*—Cooperative communication, robust communication, secrecy, smart grid, wind power generation.**

I. INTRODUCTION

Two distinctive features in the initiatives of smart grid are advanced controls and renewable energy integration. The former relies on the enhanced telecommunication infrastructure, while the latter is represented by *wind power generation* (WPG). When the attention is paid to the details of data transmission across the wind turbines, an immediate issue is the communication secrecy. The reason is obvious since the wind turbines are commonly located in open areas, no matter whether terrestrial or high seas, and the robust communication is a must. This paper investigates a representative scenario in data communications over wind farms. Two aspects will be covered. First, the practical issues involve *cooperative communications* with relays. Second, the theoretical issues are stemmed from the notion of *information-theoretic secrecy* (ITS).

Modern wireless communication technologies are undergoing evolution from the current *fifth generation* (5G) to the next generation. Besides the well-established infrastructure such as the cellular networks, the future communication systems need also support many emerging paradigms, such as *device-to-device* (D2D), *machine-to-machine* (M2M), etc. The communication layer in modern electric smart grid should embrace these technologies. Moreover, it has become a consensus that the smart grid will be significantly enhanced by the rapid development of *Internet of things* (IoT). In general, the *supervisory control and data acquisition* (SCADA) system in power grid will be strengthened by IoT. The WPG utility is of course not an exception.

Cooperative communication (also referred to as relaying communication) plays a very active role in modern wireless communication systems [1, Ch. 22]. In most systems, relay nodes can compensate the effect caused by channel fading[1]. Relay nodes can also extend the communication coverage and improve the reliability of end-to-end transmissions. Recently, there is an ever-increasing interest in the secrecy issues of cooperative communication segments. These issues are also of paramount importance in the communication layer of some components of modern smart grid, such as wind farms.

Secrecy has been considered as a fundamental issue in wireless communications. Due to the broadcasting in the open-air interface, the physical layer of wireless communications is much more vulnerable than the counterpart in wired communications. In this area, a fundamental framework of secrecy analysis is referred to as the information-theoretic secrecy (ITS). The original notion of ITS was firstly introduced by Shannon [2]. The details of ITS in the context of wireless communications can be found in [3] and [4]. Nowadays, it has been recognized that the ITS is essential for robust communications, since without it the schemes of authenticity and confidentiality may not work well.

The rest of this paper is organized as follows. In Section II, the main notations are listed. Next, in Section III, the fundamentals of robust and cooperative communications are covered, some wind farm scenarios are described, and the main contributions are summarized. Next, the link attributes are described in Section IV. Then, in Section V, the statistics of fading channels are presented. Next, in Section VI, the essentials of secrecy are reviewed. Numerical results are

[1] In wireless communications, fading is the stochastic variation of the attenuation of transmitted signals.

979-8-3503-2695-6/23/$31.00 ©2023 IEEE

presented with remarks in Section VII. Finally, the conclusion is put into Section VIII. Moreover, the proofs of the main results are included in the Appendix.

II. Notations of Secrecy System

Some primary notations and symbols are listed here for convenience.

- Tx: Legitimate transmitter
- Rx: Legitimate receiver
- Ex: Eavesdropper
- $E(\bullet)$: Mean value of its argument
- P_0: *Strictly positive secrecy capacity* (SPSC)
- U: Instantaneous *signal-to-noise ratio* (SNR) of Tx-relay link (backhaul link)
- W: Instantaneous SNR of Relay-Rx link (main access link)
- V: Instantaneous SNR of Relay-Ex link (eavesdropper access link)
- u_a, v_a, w_a: Average of U,V, and W, respectively

Other notations are defined in the places where they are firstly used..

III. Essentials and Background

A generic data exchange segment is illustrated in Fig. 1. Note that the legitimate transmitter (Tx) could be in a wind turbine or a dedicated data server.

A. Essentials of Secured Communication

Typical requirements in secured communications include integrity, authentication, and privacy [5, Ch. 11]. The present work concentrates on the privacy issue and considers the following scenario: There is a pair of legitimate transmitter (Tx) and legitimate receiver (Rx). Moreover, there is an eavesdropper (Ex). This Ex intends to intercept the data transmitted from Tx and Ex. However, the Ex is passive in that it does not send out any signals. In other words, this Ex intends to hide itself as much as possible. To focus on this specific scenario, the term "robust data exchange/communication" is adopted and used throughout this paper.

B. Essentials of Cooperative Communication

In principle, there are two fundamental protocols in cooperative communications with relays nodes (RNs): *decode-and-forward* (DF) and *amplify-and-forward* (AF) [1, Ch. 22]. Each scheme has its advantages. Analysis and practice have shown that the DF protocol can work well even in the region of low *signal-to-noise ratio* (SNR). The present study is in the context of DF.

There are several types of DF. In the present work, we adopt the *multi-hop DF* (MDF) [1, Ch. 22]. The MDF scheme is defined as follows: in the first timeslot, the source transmits, and only the relay receives. In the second timeslot, only the relay node transmits and the destination receives.

Throughout this paper, the *backhaul link* refers to the link between source and relay, and the *access link* refers to the link between relay to destinations, respectively.

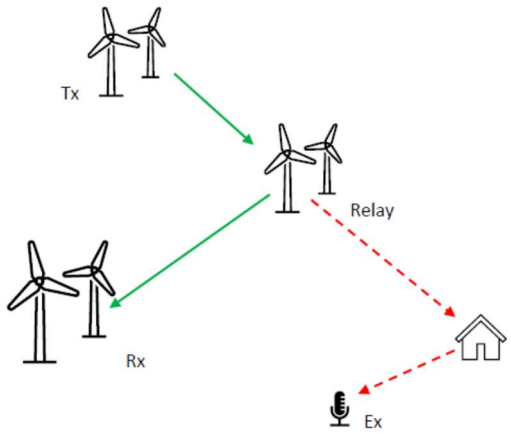

Fig. 1. A generic data exchange segment in wind farms.

C. Background of New Results

In principle, the strategy of cooperative communications with relay nodes can be implemented in either wired or wireless options. In the context of communication for wind farms, the wired option could be incorporated with the conventional approaches (telephone line, optical fiber, power line, etc.), or realized through those emerging 5G wireless technologies, such as device-to-device (D2D), machine-to-machine (M2M), or cellular networks. The main interest of this paper is in the wireless area. The signal transmission through wireless media is commonly impacted by fading, where fading is the physics phenomenon defined as variation of the attenuation of the signal. Therefore, the fading effect of wireless transmissions must be firstly investigated prior to any field deployment. Fading is typically characterized with stochastic processes and is classified to several categories [6, Ch. 2]. A fading channel in communications is a transmission channel that is impacted by fading.

Due to the complications of terrestrial locations of wind farms, there are different fading conditions for different circumstances. In the present study, we focus on the following scenario: the legitimate access link has a significant component of *line-of-sight* (LoS), while the eavesdropper access link does not. This is mainly because the eavesdropper intends to hide itself and the

availability of LoS to the wireless transmitter would be low[2].

Accordingly, two main innovative features are included in the present work. First, it is assumed that the main access link is with the *Rice* fading, while the eavesdropper's access link is subject to the *Rayleigh* fading due to potential rich multi-scattering. Second, a closed-form exact expression is derived for the *outage probability* (OP) of *secrecy capacity* (SC), rather than some lower bound or upper bound as reported in some early works [7]. Analytically, it is more difficult to deal with the *Rician* fading than *Nakagami-m* fading or Rayleigh fading [8, Ch.2]. Part of the reasons is due to the Rician distribution function involves the *Marcum Q function*, defined by an *improper integral* sharing some common features with other well-known improper functions, such as the *incomplete gamma functions*. Overall, these new features involve a great deal of mathematical complexity. However, with several sophisticated schemes, eventually some desirable closed-form solutions are found.

IV. Link Attributes

In the present work, the secrecy analysis for the MDF system with three links: the backhaul, the main access link, and the eavesdropper access link (Fig. 1). In this paradigm, the maximum achievable rate can be expressed as follows [1, eq. (22.1)]:

$$R=\frac{1}{2}\min\left\{\log_2\left(1+\frac{P_s\left|h_{sr}\right|^2}{P_n}\right),\log_2\left(1+\frac{P_r\left|h_{rd}\right|^2}{P_n}\right)\right\}, \quad (1)$$

where P_n is the noise power, while P_s and P_r are the transmission powers in source and relay, respectively. Note that $P_s/P_n=E_s/N_0$, where E_s is the transmission energy per symbol and N_0 is the one-sided power spectral density (Watts/Hz) [8, Sec. 2.2]. Moreover, h_{sr} and h_{rd} are the channel coefficients of the backhaul link and the access link, respectively. When the path-loss needs to be considered, we define the SNRs per symbols as:

$$U=\frac{P_s\left|h_{sr}\right|^2}{P_nL_{sr}^{\beta}},W=\frac{P_r\left|h_{rd}\right|^2}{P_nL_{rd}^{\beta}}. \quad (2)$$

where L_{sr} is the distance between source and relay, L_{rd} is the distance between relay and destination, and β is the path-loss exponent (usually between 1.6 and 9). Accordingly, eq. (1) can be rewritten as:

$$R=\frac{1}{2}\min\left\{\log_2(1+U),\log_2(1+W)\right\}. \quad (3)$$

First, we indicate that there is an important result in elementary mathematics: If $g(\bullet)$ is a monotonically increasing function, then

$$\min\{g(x),g(y)\}=g(\min\{x,y\}). \quad (4)$$

The proof of (4) is straightforward. Let $g(t)=\log_2(1+t)$. According to (4), we have:

$$\begin{aligned}R&=\frac{1}{2}\min\left\{\log_2(1+U),\log_2(1+W)\right\}\\&=\frac{1}{2}\min\left\{g(U),g(W)\right\}=\frac{1}{2}g(\min\{U,W\})\\&=\frac{1}{2}\log_2(1+\min\{U,W\})=\frac{1}{2}\log_2(1+X),\end{aligned} \quad (5)$$

where

$$X=\min(U,W). \quad (6)$$

Note that, in concept, the entity X is the equivalent end-to-end SNR over the two-hop between Tx and Rx.

Similarly, let Y be the equivalent end-to-end SNR over the two-hop between Tx and Ex. Then,

$$Y=\min(U,V). \quad (7)$$

According to eq. (6), the *cumulative distribution function* (CDF) of X can be written as follows:

$$\begin{aligned}F_X(x)&=\Pr(X\le x)\\&=\Pr(U\le x)+\Pr(U>x)\Pr(W\le x)\\&=F_U(x)+F_W(x)-F_U(x)F_W(x).\end{aligned} \quad (8)$$

Consequently, the *probability density function* (PDF) is:

$$\begin{aligned}f_X(x)&=f_U(x)+f_W(x)\\&\quad-f_U(x)F_W(x)-F_U(x)f_W(x).\end{aligned} \quad (9)$$

Similarly, from (7), we have:

$$F_Y(y)=F_U(y)+F_V(y)-F_U(y)F_V(y), \quad (10)$$

$$\begin{aligned}f_Y(y)&=f_U(y)+f_V(y)\\&\quad-f_U(y)F_V(y)-F_U(y)f_V(y).\end{aligned} \quad (11)$$

V. Fading Characteristics

In the concerned system, the backhaul link and the eavesdropper access link are assumed to have sufficient scattering, thus the small-scale fading can be well described by the Rayleigh distribution. The PDFs of their SNRs follow the *exponential* distribution [8, eq. (2.7)]:

$$f_U(u)=\frac{1}{u_a}\exp\left(-\frac{u}{u_a}\right), \quad (u\ge 0) \quad (12)$$

$$f_V(v)=\frac{1}{v_a}\exp\left(-\frac{v}{v_a}\right), \quad (v\ge 0) \quad (13)$$

where u_a and v_a are respectively the average of their corresponding random variables.

On the other hand, the main access link is assumed to have some components of LoS, thus the small-scale

[2] The situation can be different for non-terrestrial wind farms. For example, the eavesdropper may also have LoS to the wireless transmitter in high seas. This scenario is to be investigated in a companion paper.

fading follows the Rice distribution [8, Sec. 2.2.1.3]. Accordingly, the PDF of its SNR follows the *Rice-square* distribution:

$$f_W(w) = \frac{1}{2\sigma^2}\exp\left(-\frac{w+a^2}{2\sigma^2}\right) I_0\left(\frac{a\sqrt{w}}{\sigma^2}\right). \quad (w \geq 0) \tag{14}$$

The CDFs associated to these random variables can be respectively expressed as follows:

$$F_U(u) = 1-\exp\left(-\frac{u}{u_a}\right),\ F_V(v) = 1-\exp\left(-\frac{v}{v_a}\right),$$

and

$$F_W(w) = 1-Q\left(\frac{a}{\sigma},\frac{\sqrt{w}}{\sigma}\right), \tag{15}$$

where $Q(\bullet,\bullet)$ is the *Marcum Q function* [8, Sec. 4.2], defined by an improper integral:

$$Q(a,b) = \int_b^\infty x\exp\left(-\frac{x^2+b^2}{2}\right) I_0(ax)dx, \tag{16}$$

In which $I_0(\bullet)$ is the modified Bessel function of the first kind and order zero. Note that $E(W) = 2\sigma^2 + a^2 \overset{def.}{=} w_a$.

In the present system, the triplet (U,V,W) is supposed to be mutually independent, non-identical (heterogeneous). The non-identical attribute is an essential feature in the relay systems. For example,

$$\frac{u_a}{w_a} = \frac{E(U)}{E(W)} = \frac{P_s}{P_r}\left(\frac{L_{rd}}{L_{sr}}\right)^\beta \frac{E(|h_{sr}|^2)}{E(|h_{rd}|^2)} \neq 1. \tag{17}$$

VI. Secrecy Capacity

The present analysis is conducted in the framework established in [4]. The fading model is assumed to be quasi-static. Namely, the fading coefficients are random, but they keep constant in the time period of a codeword transmission. This notion is also known as the *block fading* in the literature of digital communications. The main metrics for this model includes the ergodic secrecy capacity, the outage probability, and the *strictly positive secrecy capacity* (SPSC). In this paper, we focus on the probability of SPSC. First, we introduce the notion of the secrecy capacity [4].

[Lemma 1]: The secrecy capacity (SC) for one realization of the SNR pair (X,Y) of the quasi-static complex fading wiretap-channel is given by:

$$H = \begin{cases} \log_2(1+X) - \log_2(1+Y), & (X > Y) \\ 0. & (X \leq Y) \end{cases} \tag{18}$$

Let $\rho > 0$ be the pre-specified secrecy rate. Then we introduce the following definition.

[Definition 2] The *outage probability* (OP) of SC is defined as:

$$P_{otg} = \Pr(H \leq \rho). \tag{19}$$

Accordingly, for $X \leq Y$, since $H = 0$ and $\rho > 0$,

$$P_{otg} = \Pr(H \leq \rho) = 1. \tag{20}$$

On the other hand, for $X > Y$,

$$P_{otg} = \Pr(H \leq \rho) = \Pr\left(\log_2\frac{1+X}{1+Y} \leq \rho\right) = \Pr\left(\ln\frac{1+X}{1+Y} \leq h\right), \tag{21}$$

where $h = \rho \ln 2$.

Consequently, the *complementary outage probability* (CPOP) of secrecy capacity is defined as:

$$P_h = \Pr(H > \rho) = 1 - P_{otg}. \tag{22}$$

In the case of non-identical Rayleigh fading, we are able to derive a closed-form expression for the CPOP of SC.

[Proposition 3] In the case of $X > Y$, the CPOP of SC can be expressed as follows:

$$P_h = \left(1+\frac{u_a}{v_a}\right)\int_0^\infty G_U[y\exp(h)+\exp(h)-1] \times G_W[y\exp(h)+\exp(h)-1] f_U(y) G_V(y) dy. \tag{23}$$

A closed-form expression is derived in Appendix.

[Definition 4] The probability of strictly positive secrecy capacity (SPSC)[3] is defined as

$$P_0 = \lim_{h\to 0} P_h. \tag{24}$$

According to the closed-form of (23) derived in the Appendix, we have:

$$P_0 = \frac{u_a+v_a}{u_a+2v_a} - \frac{u_a v_a(u_a+v_a)}{(u_a+2v_a)[u_a v_a + 2\sigma^2(u_a+2v_a)]} \times \exp\left\{-\frac{a^2(u_a+2v_a)}{u_a v_a + 2\sigma^2(u_a+2v_a)}\right\}$$

$$= \frac{u_a+v_a}{u_a+2v_a} - \frac{u_a v_a(u_a+v_a)}{(u_a+2v_a)[u_a v_a + 2\sigma^2(u_a+2v_a)]} \times \exp\left\{-\frac{2\sigma^2(u_a+2v_a)K_R}{u_a v_a + 2\sigma^2(u_a+2v_a)}\right\}, \tag{25}$$

where K_R is the *Rice factor*, defined as:

$$K_R = a^2/(2\sigma^2). \tag{26}$$

Note that K_R characterizes the power strength of the line-of-sight path to all scattered paths. It is important to

[3] For convenience, in the rest of this paper, we will simply refer the "probability of SPSC" to as "SPSC". It is important to perceive that the higher the SPSC, the better the situation is.

know the effect of K_R on SPSC. When $K=0$, the problem reduces to Rayleigh fading and we have

$$P_0 = \frac{2\sigma^2(u_a+v_a)}{u_a v_a + 2\sigma^2(u_a+2v_a)}. \quad (27)$$

Since $2\sigma^2 = w_a$ when $K_R = 0$, eq. (27) can be rewritten as follows:

$$P_0 = \frac{(u_a+v_a)w_a}{u_a v_a + (u_a+2v_a)w_a}. \quad (28)$$

On the other hand, if K_R is fairly large, then

$$P_0 \to \frac{u_a+v_a}{u_a+2v_a}. \quad (29)$$

In particular, if $v_a = u_a$, then $P_0 \to 2/3 \approx 0.667$. This figure provides a convenient limit for system design and performance evaluation.

VII. Numerical Results and Remarks

The expression of SPSC in (25) involves multiple parameters. To highlight the management effect of transmission power in (25), we introduce the ratio:

$$r_1 = \frac{u_a}{2\sigma^2} = \frac{u_a}{w_a - a^2} = \frac{P_s}{P_r}\left(\frac{L_{rb}}{L_{sr}}\right)^{\beta} \frac{E(|h_{sr}|^2)}{E(|h_{rb}|^2) - a^2}, \quad (30)$$

where L_{rb} is the distance between relay and Rx, while L_{sr} is the distance between source and relay. Note that the parameter r_1 takes into account the relative strength of the source transmission power (P_s). Similarly, we define

$$r_2 = \frac{u_a}{v_a} = \frac{P_s}{P_r}\left(\frac{L_{re}}{L_{sr}}\right)^{\beta} \frac{E(|h_{sr}|^2)}{E(|h_{re}|^2)}, \quad (31)$$

where L_{re} is the distance between relay and Ex. Since

$$\frac{r_2}{r_1} = \frac{2\sigma^2}{v_a} = \frac{E(W) - a^2}{E(V)}, \quad (32)$$

the ratio r_2 / r_1 represents the relative strength of the main access link to the eavesdropper access link. Substituting (30) and (31) into (25), we have:

$$P_0 = \frac{r_2+1}{r_2+2}\left\{1 - \frac{r_1}{(r_1+r_2+2)}\exp\left[-\frac{(r_2+2)K_R}{r_1+r_2+2}\right]\right\}. \quad (33)$$

Two representative profiles are shown in Figs. 2 and 3. First, Fig. 2 illustrates a scenario of small Rice factor ($K_r = 1.2$). If the channel condition between relay to Rx gets better (e.g., the Rice factor K_r gets larger up to 4), the performance will be improved, as shown in Fig. 3, although the benefit is more obvious when r_2 gets larger.

Overall, when the channel from relay to Rx gets deteriorated, i.e., L_{rb} increases and/or $E(|h_{rb}|^2)$ decreases, due to (30) r_1 will increase since the backhaul link from the source to relay is usually more robust. In this scenario, the SPSC P_0 will decrease, as shown in Figs. 2 and 3. However, increasing the relay power P_r will reduce r_1 and increase P_0. The trend with r_2 can be similarly explained in an inverse viewpoint[4], since a deteriorated channel from relay to Ex is favorable for SPSC.

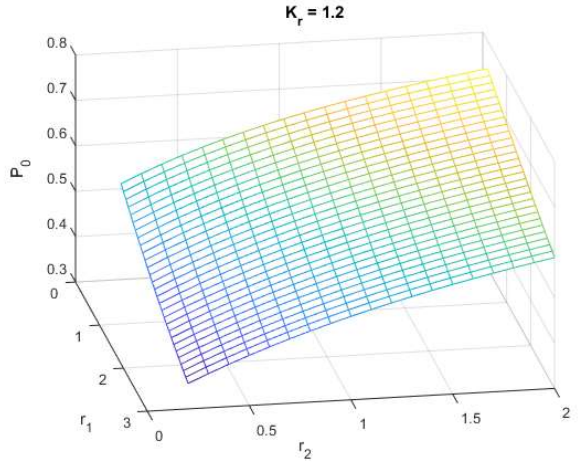

Fig. 2. SPSC of small Rice factor.

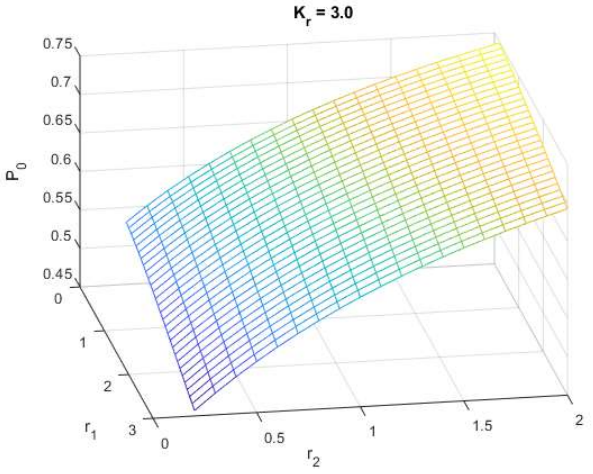

Fig. 3. SPSC of large Rice factor.

VIII. Conclusion

Robustly changing data over devices in open areas is of paramount importance in many paradigms of modern smart grid. This paper focuses on a scenario in terrestrial wind farms. Since the wind turbines in wind farms are usually deployed in the form of clusters, e.g., daisy-chain, it is quite reasonable to adopt the cooperative

[4] This can be easily seen in (33) by increasing r_2 while fixing r_1.

communication strategy with relay nodes. Given this configuration, the information secrecy is investigated.

The main analytical novelty is twofold. First, the main access link has LoS and the signal fading follows the Rice distribution. Unlike other well-known cases, the Rice variety involves the Marcum Q-function, defined by an improper integral. Its existence increases the mathematical complexity of the secrecy analysis. Secondly, rather than some approximate formulas or bounds, we derive a closed-form expression for the exact outage probability. Based on it, a benchmark metric, the probability of SPSC, can be easily evaluated. Finally, it is remarked that some analytical twists presented in the Appendix could be adopted as building-blocks and applied to other topologies of wind farms.

APPENDIX

[Derivation of the closed-form solution for eq. (23)]

In the case of $X>Y$, it follows from (21) that

$$P_h=\Pr\left(\log_2\frac{1+X}{1+Y}>\rho\right)=\Pr\left(\frac{1+X}{1+Y}>\exp(h)\right)$$
$$=\int_0^\infty\int_{y\exp(h)+\exp(h)-1}^\infty f_X(x)f_Y(y)dxdy \quad (34)$$
$$=\int_0^\infty f_Y(y)\left(\int_{y\exp(h)+\exp(h)-1}^\infty f_X(x)dx\right)dy$$
$$=\int_0^\infty f_Y(y)G_X[y\exp(h)+\exp(h)-1]dy, \quad (35)$$

where $G_X(\bullet)$ represents the *complementary cumulative distribution function* (CCDF) of X. According to (6), we have

$$G_X(x)=G_U(x)G_W(x), \quad (36)$$

while (11) can be converted to

$$f_Y(y)=f_U(y)G_V(y)+G_U(y)f_V(y). \quad (37)$$

Substituting (36) and (37) into (35), we have

$$P_h=\left(1+\frac{u_a}{v_a}\right)H_1, \quad (38)$$

$$H_1=\int_0^\infty G_U[y\exp(h)+\exp(h)-1]$$
$$\times G_W[y\exp(h)+\exp(h)-1]f_U(y)G_V(y)dy. \quad (39)$$

Incorporating the distribution functions of (U,V,W) [eqs. (12) through (15)] into (39), we have:

$$H_1=\frac{1}{u_a}\int_0^\infty\exp\left\{-\frac{1}{u_a}[y\exp(h)+\exp(h)-1]\right\}\exp\left(-\frac{y}{u_a}\right)$$
$$\times Q\left(\frac{a}{\sigma},\frac{\sqrt{y\exp(h)+\exp(h)-1}}{\sigma}\right)\exp\left(-\frac{y}{v_a}\right)dy. \quad (40)$$

Introducing the intermediate variable:

$$t=\sqrt{y\exp(h)+\exp(h)-1}, \quad (41)$$

$$H_1=\frac{2}{u_a}\exp(-h)\exp\left\{-\left(\frac{1}{u_a}+\frac{1}{v_a}\right)[\exp(-h)-1]\right\}$$
$$\times\int_0^\infty t\exp\left\{-\left(\frac{1}{u_a}+\frac{1}{v_a}\right)t^2\exp(-h)-\frac{t^2}{u_a}\right\}Q\left(\frac{a}{\sigma},\frac{t}{\sigma}\right)dt$$
$$=\frac{2}{u_a}\exp(-h)\exp\left\{-\left(\frac{1}{u_a}+\frac{1}{v_a}\right)[\exp(-h)-1]\right\}H_{11}, \quad (42)$$

where

$$H_{11}=\int_0^\infty t\exp\left\{-\left[\left(\frac{1}{u_a}+\frac{1}{v_a}\right)\exp(-h)+\frac{1}{u_a}\right]t^2\right\}Q\left(\frac{a}{\sigma},\frac{t}{\sigma}\right)dt$$
$$=\frac{u_av_a}{2[(u_a+v_a)\exp(-h)+v_a]}-\frac{(u_av_a)^2}{2[(u_a+v_a)\exp(-h)+v_a]}$$
$$\times\frac{1}{u_av_a+2\sigma^2[(u_a+v_a)\exp(-h)+v_a]}$$
$$\times\exp\left\{-\frac{a^2[(u_a+v_a)\exp(-h)+v_a]}{u_av_a+2\sigma^2[(u_a+v_a)\exp(-h)+v_a]}\right\}. \quad (43)$$

Finally, substituting (43) through (42) into (38), we obtain a closed-form of the CPOP P_h. *Q.E.D.*

REFERENCES

[1] A. F. Molisch, *Wireless Communications* (2nd Ed.), Hoboken, NJ: Wiley, 2010.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, 1949.

[3] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470-2492, 2008.

[4] M. Bloch, J. Barros, M.R.D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, 2008.

[5] A. Leon-Garcia and I. Widjaja, *Communication Networks: Fundamental Concepts and Key Architectures* (2nd Ed.), McGraw-Hill, 2004.

[6] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

[7] X. Liu, "Secrecy performance of a relaying system over non-identical fading channels," in *Proc. of Milcom* 2018.

[8] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels,* Hoboken, NJ: Wiley, 2005.